PREMIER MINISTRE
Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2023/71

Samsung TEEgris on Exynos 2200 (Version 5.0.0.0)

Paris, le 1er Février 2024

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information

Vincent STRUBEL

[ORIGINAL SIGNE]

AVERTISSEMENT

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2023/71

Nom du produit

Samsung TEEgris on Exynos 2200

Référence/version du produit

Version 5.0.0.0

Conformité à un profil de protection

GlobalPlatform Technology TEE Protection Profile
GPD_SPE_021, version 1.3

ANSSI-CC-PP-2014/01-M02, 30 juillet 2020

Critère d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL2 augmenté
AVA_VAN_AP.3

Développeur

Samsung Electronics Ltd., Co.
(16677) 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do
Korea

Commanditaire

Samsung Electronics Ltd., Co.
(16677) 129, Samsung-ro, Yeongtong-gu, Suwon-si, Gyeonggi-do
Korea

Centre d'évaluation

THALES / CNES
290 allée du Lac,
31670 Labège, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat est reconnu au niveau EAL2.

PREFACE

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- l'Agence nationale de la sécurité des systèmes d'information élabore les rapports de certification. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7) ;
- les certificats délivrés par le directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.cyber.gouv.fr.

TABLE DES MATIERES

1 Le produit

1.1 Présentation du produit

Le produit évalué est « Samsung TEEgris on Exynos 2200, Version 5.0.0.0 » développé par Samsung Electronics Ltd., Co..

Ce produit, appelé également *Samsung Secure OS*, est l'implémentation de Samsung d'un TEE (*Trusted Execution Environment*), basé sur la technologie *ARM Trust Zone*.

Le produit est utilisé sur un SoC *(System-on-Chip)* Exynos intégré dans les terminaux mobiles sous la forme d'un système d'exploitation sécurisé, permettant d'exécuter des applications de confiance dans un environnement d'exécution de confiance tout en leur apportant un ensemble de services de sécurité, tel que les services d'entreprise, la gestion de contenu (DRM – *Digital Rights Management*), la protection des données personnelles, la protection de la connectivité, les services de paiement mobile, les services d'authentification (biométrie).

Les services de sécurité du TEEgris s'appuient sur un mécanisme d'amorçage (*boot*) sécurisé qui garantit l'authenticité et l'intégrité du TEEgris OS, ainsi que sur la technologie TrustZone qui assure une isolation matérielle protégeant le monde sécurisé (*Secure World*) du monde normal (*Normal World*).

1.2 Description du produit

1.2.1 *Introduction*

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est conforme au profil de protection [PP].

1.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont :

- l'initialisation du TEE ;
- l'isolation ;
- le contrôle d'accès ;
- la cryptographie et gestion des clefs ;
- le stockage de confiance ;
- le RPMB (*Replay Protected Memory Block*) ;
- le ACSD (*Access Control Status Database*) ;
- les contremesures logicielles ;
- l'association à un appareil mobile ;
- le TUI (*Trusted User Interface*).

1.2.3 *Architecture*

Le produit est basé sur un SoC *(System-on-Chip)* Exynos 9925 et s'appuie sur la technologie ARM Trust Zone pour fournir un environnement d'exécution sécurisé pour les applications de confiance.

La figure ci-dessous explicite l'architecture du produit ; les parties grisées font partie du périmètre d'évaluation, les autres parties sont en dehors du périmètre.

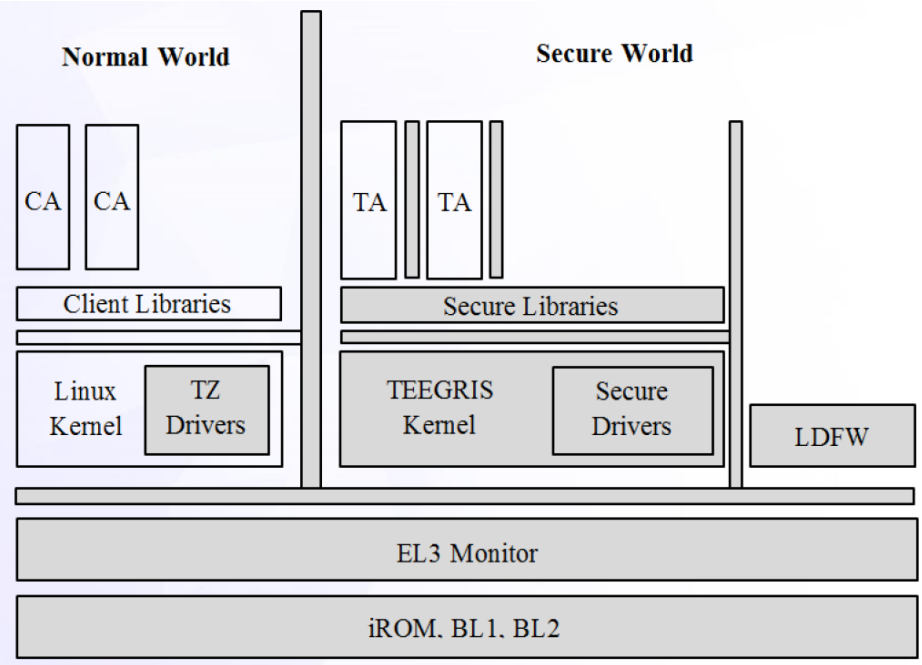

Figure 1 – Architecture du produit.

Les composants logiciels principaux de la TOE sont :

- le TEEgris *(Secure)* Kernel, qui effectue les opérations au niveau système (gestion de la mémoire, ordonnancement, gestion des périphériques) ;
- les *Secure Libraries*, qui ajoutent une couche d'abstraction au-dessus du TEEgris Kernel pour les applications de confiance. Les *Secure Librairies* implémentent les APIs Global Platform et les APIs propriétaires Samsung ;
- les modules de communication qui permettent la communication bidirectionnelle entre les deux mondes *Secure World* et *Normal World*.

La communication entre les deux mondes *Secure World* et *Normal World* est schématisée sur la figure ci-dessous.

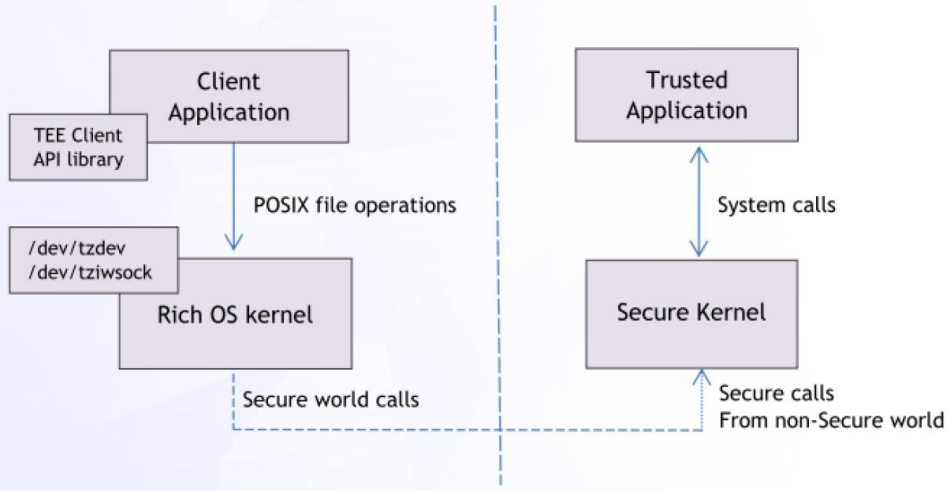

Figure 2 – Communication entre *Secure World* et *Normal World*.

1.2.4 *Identification du produit*

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par les éléments du tableau ci-après, détaillés dans la cible de sécurité [ST] à la section 2.2.2 *« TOE References »*.

Eléments de configuration		Origine
SoC	s5e9925	Samsung Electronics Co., Ltd.
Appareil mobile	Samsung Galaxy S22, S22+, S22 Ultra	
Modèle	SM-S901B, SM-S906B, SM-S908B	
DRAM	Samsung LPDDR5 8G/12G 3200MHz	
Nom commercial	Samsung *Secure OS* (TEEgris) version 5.0.0.0	
Code de ROM/*Boot*	Zagreb-SP1A-1727 sha256: 0cb293569ae1a33477f27b0acd58bd455c4d88bee53af3584facb2bc6e2f74c5	
Binaire TEE	Samsung *Secure OS Release* Version 5.0.0.0 sha256: df6e524d7accacbc722776660ffd698b023a6c55ba8cbe3b0e5cacb5b1d789db	

Binaire ATF	Zagreb-SP1A-2124V1-2125R1 sha256: 0f78b256b193620bca0f861b550371c14ac5e3b7c40d049fe6ff63a27d3d0512	

L'utilisateur peut vérifier la version du SoC de l'appareil mobile par la procédure suivante :

- D'abord identifier la référence de l'appareil mobile dans le menu *« Settings »* > *« About phone »* > *« Model name »*
- Ensuite utiliser cette référence de l'appareil mobile pour identifier la référence du SoC à l'aide des sources suivantes :
  - https://semiconductor.samsung.com/us/processor/mobile-processor/
  - https://semiconductor.samsung.com/us/processor/showcase/smartphone

1.2.5 *Cycle de vie*

Le cycle de vie du produit est décrit au chapitre 3.3 de [ST].

Le cycle de vie implique les deux divisions suivantes du développeur :

- Pour la fabrication du SoC : Samsung Electronics Co., Ltd, *Device Solutions, System LSI Business ;*
- Pour la fabrication de l'OS de confiance, et pour le développement et la fabrication de l'appareil mobile : Samsung Electronics Co., Ltd, *Device eXperience, Mobile eXperience (MX) Business*

Le cycle de vie comporte les sept phases suivantes :

- Conception du matériel et du *firmware* du TEE ;
- Fabrication du matériel du *SoC* ;
- Conception du logiciel (TEE + REE) ;
- Fabrication du logiciel du TEE ;
- Intégration du TEE dans l'appareil mobile final ;
- Fabrication de l'appareil mobile (initialisation et personnalisation du TEE avant livraison) ;
- Utilisation de l'appareil mobile.

1.2.6 *Configuration évaluée*

Le certificat porte sur le produit identifié dans la cible de sécurité [ST] au chapitre 2.2 *« TOE identification »*, dans ses configurations permises par les [GUIDES]. Au regard du cycle de vie, le certificat porte sur le produit livré à l'issue de la phase 6.

2 L'évaluation

2.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [CC], et à la méthodologie d'évaluation définie dans le manuel [CEM].

2.2 Travaux d'évaluation

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 11 décembre 2023, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse a identifié des non-conformités par rapport aux référentiels [ANSSI Crypto] et [SOG-IS Crypto]. Elles ont été prises en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé. L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme aux référentiels [ANSSI Crypto] et [SOG-IS Crypto], pour les mécanismes cryptographiques qui le permettent.

2.4 Analyse du générateur d'aléa

Le produit comporte un générateur d'aléa qui a fait l'objet d'une analyse conformément à la procédure [CRY-P-01].

Cette analyse n'a pas identifié de non-conformité par rapport aux référentiels [ANSSI Crypto] et [SOG-IS Crypto].

L'analyse de vulnérabilité indépendante réalisée par l'évaluateur n'a pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau d'attaquant visé.

3 La certification

3.1 Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé.

3.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES].

3.3 Reconnaissance du certificat

3.3.1 *Reconnaissance européenne (SOG-IS)*

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour certains équipements matériels avec boîtiers sécurisés, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2 *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[2] , des certificats Critères Communs.

La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.eu.

[2] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

ANNEXE A. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - *Samsung TEEgris Security Target on Exynos 2200*, référence Samsung_TEEgris_*Security_Target*_v2.10, version 2.10, 9 août 2023.
[RTE]	Rapport technique d'évaluation : - *Evaluation Technical Report - SANGHA*, référence TEEgris5-S22_ETR, version 1.5, 9 janvier 2024.
[CONF]	Liste de configuration du produit : – *Samsung TEEgris Lifecycle and Configuration*, version 1.4, 20 juillet 2023
[GUIDES]	Guide d'utilisation du produit : - *Samsung TEEgris Overview and Guidance*, version 1.5 TEEgris v5.0.0 , 9 août 2023.
[PP]	GlobalPlatform Technology TEE *Protection Profile*, GPD_SPE_021 version 1.3, ANSSI-CC-PP-2014/01-M02, 30 juillet 2020

ANNEXE B. Références liées à la certification

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER-P-01]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.0.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[CC]	*Common Criteria for Information Technology Security Evaluation:* - *Part 1 : Introduction and general model*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001 ; - *Part 2 : Security functional components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002 ; - *Part 3 : Security assurance components*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	*Common Methodology for Information Technology Security Evaluation: Evaluation Methodology*, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[CCRA]	*Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security*, 2 juillet 2014.
[SOG-IS]	*Mutual Recognition Agreement of Information Technology Security Evaluation Certificates*, version 3.0, 8 janvier 2010, Management Committee.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.
[SOG-IS Crypto]	*SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms*, version 1.2, janvier 2020.
[AIS20/31]	*A proposal for: Functionality classes for random number generators, AIS20/AIS31*, version 2.0, 18 septembre 2011, BSI (*Bundesamt für Sicherheit in der Informationstechnik*).